

VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Absolvování individuální odborné praxe

Individual Professional Practice in the Company

Zadání bakalářské práce

Student: **Vendula Filipcová**
Studijní program: B2647 Informační a komunikační technologie
Studijní obor: 2601R013 Telekomunikační technika
Téma: **Absolvování individuální odborné praxe**
Individual Professional Practice in the Company

Jazyk vypracování: čeština

Zásady pro vypracování:

1. Student vykoná individuální praxi ve firmě: Tieto Czech s.r.o.
2. Struktura závěrečné zprávy:
 - a. Popis odborného zaměření firmy, u které student vykonal odbornou praxi a popis pracovního zařazení studenta
 - b. Seznam úkolů zadaných studentovi v průběhu odborné praxe s vyjádřením jejich časové náročnosti
 - c. Zvolený postup řešení zadaných úkolů
 - d. Teoretické a praktické znalosti a dovednosti získané v průběhu studia uplatněné studentem v průběhu odborné praxe
 - e. Znalosti či dovednosti scházející studentovi v průběhu odborné praxe
 - f. Dosažené výsledky v průběhu odborné praxe a její celkové zhodnocení

Seznam doporučené odborné literatury:

Podle pokynů konzultanta, který vedl odbornou praxi studenta


Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Zdeňka Chmelíková, Ph.D.**


Konzultant bakalářské práce: Ing. Radim Koch

Datum zadání: 01.09.2016

Datum odevzdání: 28.04.2017


doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry




prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlašuji, že jsem tuto bakalářskou práci vypracovala samostatně. Uvedla jsem všechny literární prameny a publikace, ze kterých jsem čerpala.

V Ostravě 18. dubna 2017

Vendula Filipcová
.....

Souhlasím se zveřejněním této bakalářské práce dle požadavků čl. 26, odst. 9 Studijního a zkušebního řádu pro studium v bakalářských programech VŠB-TU Ostrava.

V Ostravě 18. dubna 2017

Tieto Czech s.r.o.
28. října 3346/91
702 00 Ostrava - Moravská Ostrava
..... IČO 64608051 DIČ CZ64608051

Ráda bych poděkovala celému Tieto Exchange týmu, jmenovitě pak Ing. Jaroslavu Zemánkovi, Ing. Radimu Kochovi a Tomášovi Václavíkovi za pomoc při vytváření mé bakalářské práce, poskytnutí odborných informací, korekci a příjemný pracovní kolektiv. Dále děkuji paní proděkance Ing. Zdeňce Chmelíkové, Ph.D. za konzultace k bakalářské práci a poskytnutí užitečných rad pro její vypracování.

Abstrakt

Praktická bakalářská práce je zaměřena na problematiku Exchange prostředí, které se s novými technologiemi a možnostmi vyvíjí. Zaměřuji se na dvě rozdílná řešení emailové komunikace ve firmách a to na lokální Microsoft Exchange On-Premise a cloudové řešení Microsoft Office 365. Řeším jejich rozdílnost, výhody a nevýhody a v neposlední řadě také jejich implementaci. Přechody do cloudových systémů jsou dnes velice aktuální a řešené téma ve firmách poskytovatelů, proto jsem si tento okruh telekomunikací vybrala jako klíčový. Pro svou bakalářskou práci jsem navrhla schémata obou řešení, abych nejlépe demonstrovala rozdíly v topologii a popsala tak velkou část mé práce na projektu.

Cloud, čili možnost přistupovat ke svým datům a aplikacím kdekoliv z internetu, vyžaduje stále více velkých korporací. Velkou roli zde hrají finanční prostředky, které se promítají do firemních finančních plánů. Lokální On-Premise řešení je velice náročné na prvotní finance a začínající firmy dnes skoro jednoznačně volí služby formou předplatného, tedy cloud. Základními aspekty přechodu tedy migrace do Office 365, jsou finanční náklady v závislosti na čase, stabilita daného řešení nebo zabezpečení a ochrana dat.

Díky odborné bakalářské praxi jsem se dostala jak k řešení výše zmíněných komplexních projektů, tak k řešení jednotlivých problémů, proto do práce zapojím také dílčí technologie, se kterými jsem se setkala a pracovala s nimi, jako jsou bezpečnostní emailové brány nebo Exchange Management Shell.

Klíčová slova: Odborná praxe, Microsoft Exchange Server, Microsoft Office 365, emailová komunikace, cloudová řešení, projekt, migrace, Active Directory, bezpečnostní emailová brána a ochrana uživatelů, bezpečnost, topologie serverů, Exchange Management Shell.

Abstract

The practical bachelor thesis is primary about the Exchange environment which is evolved with new technologies and technical possibilities. I focused my attention on two different solutions of email communication in the companies which are local solution Microsoft Exchange On-Premise and cloud solution Microsoft Office 365. I am devoting with their differences, pros, cons and also implementation. Migrations to the cloud systems are very relevant topic nowadays in the providers' companies and this is the reason why I choose this telecommunication branch for my thesis. I created sample schemes of solutions to explain differences between both and I described a great part of my work on the project.

The cloud solutions become more intended in the companies because of possibility to access data and applications anywhere from the Internet. A big role is played by the funds which are reflected in the financial plans. A local On-Premise solution may be expensive and that is reason why cloud services by subscription are chosen by starting companies. The basic aspects of migration itself are costs depending on the time, stability, security and data protection or sustainability.

Thanks to the Individual Professional Practice in the Company I worked both on the project and individual problems. My thesis includes also partial technologies I worked with as messaging secure gateways or scripting language Exchange Management Shell.

Key Words: Professional work experience, Microsoft Exchange Server, Microsoft Office 365, email communication, cloud solutions, project, migration, Active Directory, messaging secure gateway and user protection, safety, topology of the servers, Exchange Management Shell.

Obsah

Seznam použitých zkratk a symbolů	10
Seznam obrázků	11
Seznam tabulek	12
Seznam výpisů zdrojového kódu	13
Úvod	14
1 O firmě	15
1.1 Tieto v České republice	15
1.2 Organizace a struktura	15
2 O Exchange týmu	16
2.1 Popis práce	16
2.2 Zařazení v týmu v rámci praxe	16
3 Microsoft Exchange vs. Office 365	18
3.1 Uvedení do problematiky	18
3.2 Definice Exchange Serveru	19
3.3 Microsoft Exchange Server	19
3.4 Microsoft Office 365 – Cloudové řešení	21
3.5 Srovnání topologií Microsoft Exchange Server a Office 365	23
3.6 Výhody a nevýhody	27
4 Proces migrace jako moje práce	30
4.1 Typy migrací	30
4.2 Fázová migrace	31
5 Bezpečnost a ochrana dat	38
5.1 Bezpečnostní emailová brána	38
5.2 Práce s bezpečnostní emailovou branou	38
6 Další úkoly v rámci odborné praxe	40
6.1 Out of office	40
6.2 Auto-mapping	41
6.3 Přístupová oprávnění	41
6.4 Úložiště	42

7	Zhodnocení znalostí a dovedností	44
7.1	Znalosti získané v průběhu studia	44
7.2	Znalosti scházející v průběhu odborné praxe	44
7.3	Celkové zhodnocení	45
	Závěr	46
	Literatura	47

Seznam použitých zkratk a symbolů

AD	– Active Directory
AD FS	– Active Directory Federation Services
CS	– Continuous Service
CSV	– Comma-separated values
DAG	– Database Availability Group
DirSync	– Directory Synchronization
DMZ	– Demilitarized Zone
DNS	– Domain Name System
EAC	– Exchange Admin Center
EAS	– Exchange ActiveSync
EMS	– Exchange Management Shell
EOP	– Exchange Online Protection
EWS	– Exchange Web Services
HD	– High Definition
HTML	– HyperText Markup Language
HTTP	– Hypertext Transfer Protocol
IMAP	– Internet Message Access Protocol
IT	– Information Technology (Informační Technologie)
MAPI	– Messaging Application Programming Interface
MS	– Microsoft
MX	– Mail Exchange
O365	– Office 365
OS	– Operating System (Operační Systém)
POP3	– Post Office Protocol
PST	– Personal Storage Table
SMG	– Symantec Messaging Gateway
SMTP	– Simple Mail Transfer Protocol
SW	– Software
TCP	– Transmission Control Protocol
TXT	– Textový soubor
UcaaS	– Unified Communications as a Service
VoIP	– Voice over Internet Protocol
VPN	– Virtual Private Network (Virtuální privátní síť)
XHTML	– eXtensible HyperText Markup Language

Seznam obrázků

1	Centrum pro správu Exchange (Exchange Admin Center)	20
2	Topologie prostředí Microsoft Exchange On-Premise	24
3	Topologie prostředí Microsoft Office 365 s On-Premise AD	26
4	Office 365 administrátorský portál	32
5	Přidání TXT a MX záznamu na DNS server	33
6	Přidání rolí a funkcí na DNS serveru	34
7	Microsoft Azure Active Directory Connect	35

Seznam tabulek

1	Přenesená a zaniklá data při migraci	36
2	Přehled zpráv s hrozbami redukoványi SMG za 30 dní	39

Seznam výpisů zdrojového kódu

1	Přihlášení na Microsoft server	22
2	Přihlášení do PS pro Azure AD	23
3	CSV soubor	36
4	Nastavení „Send-As“ oprávnění	37
5	Nastavení out of office	40
6	Nastavení auto-mapping	41
7	Výpis sdílených schránek	42
8	Přiřazení práv	42
9	Výpis kvót	43

Úvod

K volbě praktické bakalářské práce mne motivovalo propojení převážně teoretických znalostí získaných ze studia s pracovními zkušenostmi. Díky výběru praxe v mezinárodní firmě jsem měla možnost pracovat v týmu specialistů a zabývat se podrobně technickým okruhem emailové komunikace.

V prvních kapitolách bakalářské práce uvádím základní informace a odborný popis zaměření firmy Tieto, kde jsem vykonávala praxi. Zařadila jsem se do Exchange týmu, který řeší nejen interní emailový provoz, ale stará se také o veškeré zákazníky využívající služeb emailové komunikace, což zahrnuje správu desítek tisíc uživatelů. Exchange tým řeší dílčí problémy s doručováním služby zákazníkovi, technickou podporu, realizaci a plánování projektů nebo implementaci nových produktů.

Dále rozepisuji důležitou problematiku k tématu emailové komunikace, kterou jsem studovala a učila se během odborné praxe, zejména pak popisuji dvě rozdílná řešení pro implementaci Exchange prostředí – Microsoft Exchange On-Premise lokální řešení a inovativní cloudové řešení Office 365. Navrhla jsem topologie, které demonstrují rozdílnost a způsob implementace. Uvádím rozdílnosti mezi oběma řešeními a to především proto, že jsem si jako hlavní projekt pro svou bakalářskou práci vybrala migraci. V mém případě migrace znamená, přesun mezi výše zmíněnými prostředími v rámci jedné firmy. Jedná se o IT projekt, který má několik částí a mnoho technických postupů, a jehož průběh je kvůli komplexnosti rozložen do několika týdenního plánu. V bakalářské práci se věnuji obecně nejdůležitějším bodům migrace, nikoliv detailnímu postupu a popisuji použité technologie a kroky, které jsem v daném případě volila. V neposlední řadě se věnuji otázce bezpečnosti a ochrany dat uživatelů.

S bezpečností se pojí i další dílčí úkoly, které jsem na odborné praxi mimo projekt vykonávala. Seznámila jsem se s fungováním bezpečnostních emailových bran a s jejich správou, která je potřeba v každé funkční Exchange topologii. Jednu z posledních kapitol jsem věnovala administrátorskému nástroji Exchange Management Shell, který je základním příkazovým nástrojem pro správu jakéhokoliv Exchange prostředí, a který jsem využívala nejen při řešení jednotlivých úkolů, ale také při migraci.

V poslední kapitole jsem zhodnotila své znalosti získané v průběhu studia a znalosti scházející v průběhu praxe. Ačkoliv pro mne byly odborné informace z oblasti Exchange Serverů a cloud computingu z velké části nové, měla jsem široký přehled o používaných technologiích, serverech, zabezpečení a šifrování či IP protokolech právě díky studiu na vysoké škole.

1 O firmě

Tieto je největší severoevropská IT společnost, poskytující komplexní IT servis. Zajišťuje také služby v oblasti vývoje produktů pro firmy působící v odvětví komunikací a integrovaných technologií. Na základě svých znalostí, technologických vizí a inovativního myšlení se společnost Tieto aktivně snaží inspirovat a zapojit své zákazníky do hledání nových způsobů, jak zefektivnit jejich podnikatelskou činnost. Tieto spojuje globální možnosti s přítomností na lokálních trzích a zároveň staví na svém severském odkazu. Společnost Tieto se sídlem ve finských Helsinkách zaměstnává přes 13 000 expertů ve 20 zemích světa. Obrat činí přibližně 1,5 miliard eur.[1]

1.1 Tieto v České republice

Do České republiky společnost Tieto vstoupila v roce 2001 a v roce 2004 otevřela své softwarové centrum v Ostravě. S více než 2 200 zaměstnanci je jedním z největších zaměstnavatelů v oblasti IT služeb v České republice a největším v Moravskoslezském kraji. Z hlediska počtu kmenových zaměstnanců je česká pobočka třetí největší pobočkou Tieto korporace na světě. První dvě místa zaujímají mateřské země Finsko a Švédsko.[1]

1.2 Organizace a struktura

Tieto má poměrně složitou vnitřní strukturu, která je rozdělena do několika vrstev a mnoha technicky i netechnicky zaměřených týmů. Tieto z velké části zabezpečuje nepřetržitou technickou podporu pro všechny své zákazníky, proto jednu z největších skupin zaměstnanců Tietu tvoří *Service Desk*. Tito lidé se starají o komunikaci se zákazníkem, zjišťují potřebné informace k požadavkům uživatelů a dokáží řešit jednoduché technické problémy. Eliminují tak velké množství práce, která by se jinak dostávala k technickým specialistům, kteří řeší závažnější a složitější problémy. Když *Service Desk* nemá dostatečnou kompetenci či znalost k řešení, pošle požadavek dále. Tyto složité požadavky a problémy řeší specialisté v daném technickém okruhu, podle kterých jsou týmy rozděleny.

Specialisté se zabývají i složitými případy, mají veškeré administrátorské přístupy a znají problematiku svého technického okruhu. Mohou nést zodpovědnost za určitého zákazníka či zákazníky, řešit individuální problémy a podílet se na vývoji nabízených služeb. Součástí těchto týmů jsou vedle specialistů také architekti. Architekti již neřeší problémy jednotlivých uživatelů, ale mají za úkol globální komunikaci s celými firmami, mají odpovědnost za kompletní technické odvětví, ve kterém pracují. Navrhují vhodná řešení a podílejí se na důležitých projektech. Každý technický tým je veden manažerem, který řeší organizační záležitosti týmu.

Vedle technicky zaměřených týmů jsou v Tietu také netechnické skupiny lidí, kteří zajišťují finance, náborů nebo mimopracovní aktivity v rámci firmy. Tieto disponuje také množstvím manažerských pozic, nad kterými stojí personální a generální ředitel.

2 O Exchange týmu

V rámci praktické bakalářské práce jsem pracovala ve firmě Tieto Czech s.r.o. na pozici technického specialisty v Exchange teamu. Exchange team nese zodpovědnost za veškeré dění ohledně emailové komunikace, správy a údržby Exchange serverů či emailových bezpečnostních bran. Dále řeší problémy uživatelů a zajišťuje podporu plynulého a bezchybného provozu. Emailová komunikace je ve firmách důležitým telekomunikačním a informativním prostředkem, který sebou nese řadu dalších funkcionalit. Je to komplexní technický okruh, důležitý pro fungování významné většiny firem.

2.1 Popis práce

Exchange team nebo také Mail team mohou rozdělit do dvou skupin technických specialistů a architektů, abych lépe ilustrovala náplň práce celého týmu.

První skupinou jsou Servis Architekti, kteří se účastní projektů, jejichž cílem je buď implementace emailového prostředí pro nové zákazníky nebo přechod našich stávajících zákazníků na vyšší verzi produktu Microsoft Exchange. Jsou zodpovědní za kompletní instalaci SW (Software) na Exchange Server, konfiguraci serverů, databázových úložišť, webových služeb (Autodiscover, EWS, OAB, Outlook Anywhere, MAPI over HTTP, ActiveSync) a síťových služeb (FW, F5, DNS). Součástí projektů je rovněž zajištění funkcí antispamové ochrany. Zde je k dispozici antispamové řešení Symantec Bright Mail Gateway nebo StaySecure, které provozuje službu na svých serverech. V neposlední řadě architekti konfigurují monitorovací systémy a reportovací nástroje, vytvářejí technickou dokumentaci a instrukce pro Service Desk. Jejich práce na projektu končí přesunem služby do CS (Continuous Service).

Druhá skupina je tvořena Servis Administrátory, kteří řeší problémy spojené s doručováním služby zákazníkovi v požadovaném čase a kvalitě, po přesunutí služby do CS analyzují abnormality systému, monitorují výkonnost emailového systému, dostupnost služby a systémových zdrojů. Dále zajišťují podporu koncovým uživatelům, řeší problémy s připojením poštovních klientů a mobilních zařízení a podílí se na vytváření znalostní báze. Součástí administrace je pravidelná údržba emailového prostředí, zejména instalace aktualizací a hotfixů. Nejčastěji používané administrační nástroje jsou Exchange Admin center, PowerShell (Exchange Management Shell), Telnet, Nslookup, Microsoft Remote connectivity Analyzer, Exchange environment report a další.

2.2 Zařazení v týmu v rámci praxe

V Exchange týmu jsem pracovala na pozici technického specialisty, měla jsem stejná administrátorská práva a přístupy na servery firem jako ostatní kolegové. Díky tomu jsem mohla vykonávat plnohodnotnou práci pro firmu a získávat tak zkušenosti v okruhu emailové komunikace. Mou pracovní náplní byla podpora uživatelů na technické úrovni, řešení jednotlivých i globálních

problémů, práce v Exchange server prostředích včetně používání nástroje PowerShell, administrátorská orientace v antispamových emailových branách a jejich nastavení a v neposlední řadě studium novodobého řešení Microsoft Office 365. Podílela jsem se na kompletním přechodu firmy z řešení On-Premise Exchange Server 2007 na cloudové online řešení Office 365, což jsem pojala jako hlavní téma mé praktické bakalářské práce. Jedná se o rozsáhlý projekt, který zahrnuje spoustu informací a veškeré znalosti o Exchange.

3 Microsoft Exchange vs. Office 365

V této kapitole se budu věnovat rozdílům mezi dvěma řešeními provozu emailové komunikace. Nejprve uvedu jakou má Exchange Server důležitost a jaká je aktuální situace pro firmu, kde jsem vykonávala praxi. Dále popíšu obě řešení, včetně celkových schémat, která jsem navrhla pro nejlepší demonstraci rozdílů. Následně srovnám tato řešení a zaměřím se na výhody a nevýhody použití On-Premise a cloudu v rámci emailové komunikace.

3.1 Uvedení do problematiky

Tieto pro své zákazníky nabízí mnoho služeb z různých odvětví informatiky a telekomunikací. Konkrétně Exchange tým zajišťuje veškeré technické služby týkající se emailové komunikace.

Emailová, nebo také elektronická komunikace patří dnes neodmyslitelně ke každé firmě či organizaci. Nejpoužívanějším softwarovým řešením v rámci firmy je Exchange server, který umožňuje přijímání a odesílání emailů mezi uživateli nebo mezi uživateli a objekty. Tieto poskytuje servery ve svých datacentrech, zajišťuje na nich veškerou funkčnost smlouveného softwaru a jeho nepřetržitou údržbu. V minulosti se jednalo, až na drobné výjimky, zejména o řešení Microsoft Exchange Server, s nímž se pojí Microsoft Outlook nebo jiný emailový klient. Microsoft Exchange Server jako produkt vznikl v roce 1996 a stále se vyvíjí. Během bezmála dvaceti let vydal Microsoft 9 úplných verzí Exchange Serveru, přičemž vycházely i doplňující aktualizace, které odstraňují nedostatky v nových verzích.

Zlom přišel v roce 2011, kdy Microsoft uvedl na trh Office 365 pro firmy. O365 (Office 365) je balík služeb a softwaru, který funguje na principu předplatného. Majitelem fyzických serverů je již samotný Microsoft, a poskytuje takzvaně cloudové řešení. U takového řešení si zákazník nekupuje žádné fyzické servery a o veškerý provoz se stará poskytovatel. Cloudová řešení se těší stále větší oblibě, a proto je postupem času do své nabídky služeb uvedlo také Tieto. Než společnost Tieto do své nabídky zahrnula řešení od Microsoftu, předcházelo tomu několik vlastních pokusů. V roce 2011 vznikl v Tietu vlastní cloud UcaaS (Unified Communications as a Service), který ačkoliv funguje dodnes, bude brzy zrušen. Další pokus o vlastní cloud, postavený na TPC (Tieto Private Cloud), proběhl ještě o tři roky později. Projekt byl však utlačen z důvodu masivního nástupu O365, který byl pro zákazníky neporovnatelně cenově dostupnější. Od tohoto momentu se zákazníkům začíná nabízet řešení O365, včetně migrací u zákazníků, kteří doposud vyžívají Microsoft Exchange Server a služby s ním spojené.

První zákazník Tietu přecházel z řešení Microsoft Exchange Server do O365 na přelomu dubna a května 2015. O cloudová řešení je stále větší zájem a to z velké části kvůli snížení režijních nákladů.

3.2 Definice Exchange Serveru

Exchange Server lze definovat jedním slovem – Groupware – nebo také systémy pro podporu spolupráce. Groupware je označení pro počítačové nástroje, které pomáhají ke spolupráci pracovníků ve firmě (workgroups). V případě Exchange serveru se jedná například o plánování schůzek, emailovou komunikaci, sdílení dokumentů a souborů, služby VoIP (Voice over Internet Protocol), elektronický zpravodaj ve firmách a další.

Primární funkcí Exchange serveru je emailová komunikace, která je zde využívána ze všeho nejvíce. Přesto má Exchange server další funkce, jako je například kalendář a plánování schůzek, adresář kontaktů, mobilní emailová komunikace, zvukový email, seznamy úkolů a desítky dalších včetně funkcí pro administrátory.

Exchange server funguje na principu klient – server, je to jednoduchý koncept, kde Exchange Server poskytuje veškeré zmíněné funkce. Uživatelé se připojují ke svým emailovým schránkám na Exchange server přes emailového klienta. Pro připojení lze využít různé typy klientů například webový Outlook Web App, ActiveSync pro chytré mobilní telefony či tablety nebo nejznámější Outlook. Dále existují klienti třetích stran pro přístup k emailové poště například Unibox nebo Postbox.

3.3 Microsoft Exchange Server

Jedná se o softwarový produkt společnosti Microsoft, který slouží k příjmu a odesílání emailových zpráv, ke správě kalendáře nebo sdílení veřejných složek. Je možné jej instalovat výhradně na operační systém Windows Server. Exchange server má úzkou spojitost s Active Directory a musí být instalován na doménový server.

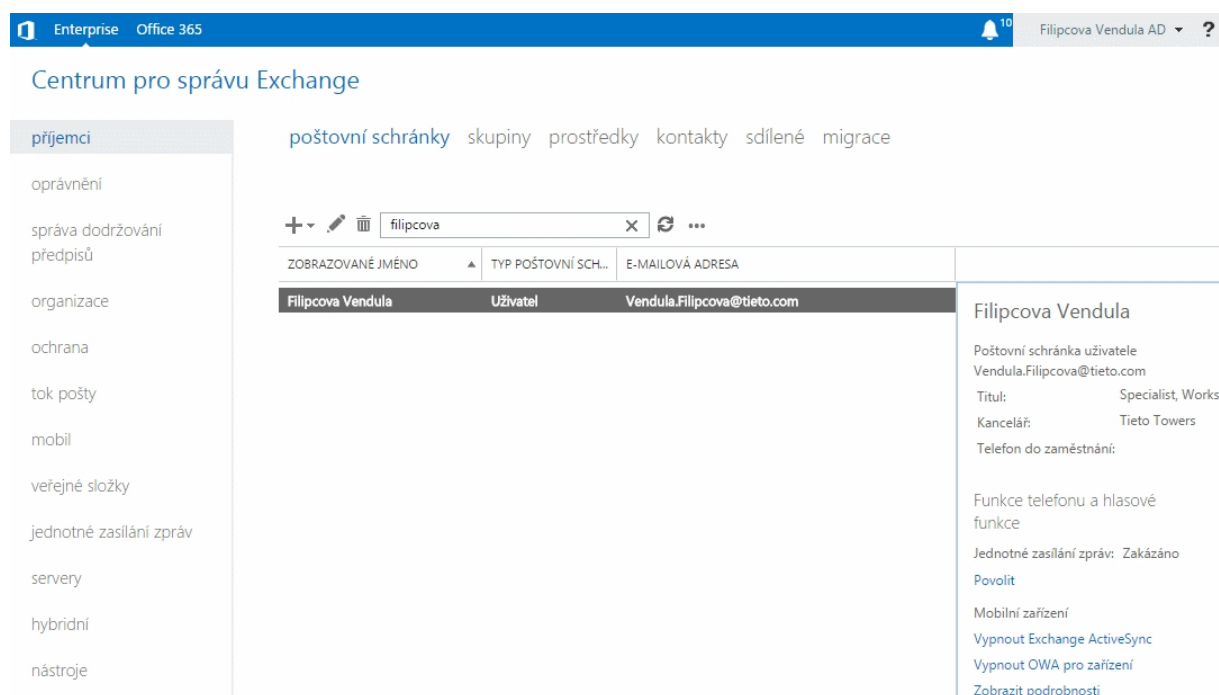
První verze pojmenována Exchange Server 4.0 byla uvedena na trh v dubnu 1996, jednalo se již o produkt založený na principu klient – server. Pracoval na systému X.400 a využíval protokolu MAPI (Messaging Application Programming Interface). S dalšími verzemi softwaru se zvyšovaly nároky uživatelů a značně se vyvíjel IT obor. V následujících verzích byl postupně nahrazen původní systém X.400 za Microsoft Active Directory a byl rozšířen o podporu dnes používaných protokolů POP3 (Post Office Protocol), IMAP (Internet Message Access Protocol), SMTP (Simple Mail Transfer Protocol) a EAS (Exchange ActiveSync).

S Microsoft Exchange serverem je úzce svázán e-mailový klient Microsoft Outlook, který slouží nejen jako *emailová aplikace*, ale také ke sdílení pošty nebo jako kalendář k organizaci schůzek. První verze pojmenovaná Outlook for MS-DOS byla dostupná společně s Exchange Serverem 5.5.

V rámci odborné praxe jsem se nejčastěji setkávala s verzemi Exchange Server 2007, Exchange Server 2010, Exchange Server 2013 a Exchange Server 2016 (Office 365). Všechny vydané verze a jejich data vydání jsou pak následující:

Exchange Server 4.0, 1. duben 1996
 Exchange Server 5.0, 23. května 1997
 Exchange Server 5.5, 3. února 1998
 Exchange Server 2000, 29. listopadu 2000
 Exchange Server 2003, 28. září 2003
 Exchange Server 2007, 8. března 2007
Exchange Server 2010, 9. listopadu 2009
Exchange Server 2013, 3. prosince 2012
Exchange Server 2016, 1. října 2015. [2]

Všechny verze Microsoft Exchange Server jsou poskytovány takzvaně On-Premise nebo na virtuálních serverech, s výjimkou verze Exchange Server 2016, která zahrnuje Office Online neboli zmíněný Office 365. U řešení On-Premise si zákazník musí zajistit vlastní hardware (fyzické servery) i software (Microsoft Exchange Server), který zaplatí jednorázově za licenci. Zákazník dále platí za konektivitu a technickou údržbu serverů, které může mít umístěné ve vlastní firmě či v datacentrech Tieto. Hlavním administrátorským portálem pro správu je EAC (Exchange Admin Center) na obrázku 1.



Obrázek 1: Centrum pro správu Exchange (Exchange Admin Center)

3.3.1 Serverové role

Role Exchange serveru existují proto, aby každý server mohl vykonávat nějakou z rolí a tak se mezi ně jednoduše rozložila zátěž. V prvních verzích produktu Exchange Serveru bylo vyžadováno větší množství hardwaru, jelikož servery nebyly tak výkonné, jak je tomu dnes. S každou novou verzí se struktura zjednodušuje a upravuje.

Role Exchange Serveru 2007/2010

- Mailbox Server (databáze emailových schránek a veřejných složek)
- Client Access Server (klientské připojení pro OWA (Outlook Web App), EWS (Exchange Web Services), ActiveSync či spojení Outlooku s mailbox serverem)
- Hub Transport Server (tok zprávy – přijímání a odesílání)
- Edge Transport Server (zabezpečení zpráv a filtrace spamu)
- Unified Messaging (zvukové email a Outlook Voice Access)

Role Exchange Serveru 2013

- Mailbox Server (role Mailbox Serveru, Hub Transport Serveru a Unified Messaging)
- Client Access Server (klientské připojení pro OWA, EWS, ActiveSync či spojení Outlooku s mailbox serverem)
- Edge Transport Server (zabezpečení zpráv a filtrace spamu)

Role Exchange Serveru 2016

Rozložení Exchange Serveru 2016 se vrací zpět k verzi Exchange Server 2003, jež měl pouze dvě role a to Front-end Server, který zastával funkci pro tok emailové komunikace a Back-end Server, jež držel databáze emailových schránek a veřejných složek. Je to první verze Microsoft Exchange Serveru, kdy se klienti připojují přímo na Mailbox server.

- Mailbox Server (veškeré služby spojené s emailovými schránkami a klientským přístupem)
- Edge Transport Server (veškeré služby spojené s tokem zprávy, zabezpečením a Unified Messaging)

3.4 Microsoft Office 365 – Cloudové řešení

Jde o relativně nový koncept, který v roce 2011 uvedl Microsoft do svého portfolia. Exchange Office 365 bývá často nazýván také jako Exchange Online. Je to soubor cloudového softwaru vytvořený společností Microsoft, který funguje na systému předplatného – obecně nazýváno cloud computing. Cloud computing je moderní koncept používání počítačových technologií, kdy

poskytovatel služby nebo aplikace vlastní veškerý potřebný HW (hardware), tedy především servery. Uživatelé ke službě přistupují vzdáleně odkudkoliv z internetu. Uživatelé hradí pravidelně takzvaně předplatné za využívání služby a nestarají se o údržbu ani správu z technického hlediska, jak tomu je u lokálních řešení.

V případě Office 365 jsou pro uživatele i firmy navrženy různé softwarové balíky, které obsahují aplikace a služby Microsoftu. Zákazník si může vybrat od základního balíku až po komplexní, který obsahuje všechny produkty. Každý zákazník Office 365, ať už jednotlivec nebo firma hradí měsíční předplatné balíku, který je pro něj nejvhodnější, přičemž firmy platí poskytovateli za každého jednoho aktivního zaměstnance, kterému je přiřazena licence. Ceny licencí se orientačně pohybují mezi 4 až 10 eury za jednoho uživatele. [3]

V typickém Business předplatném Office 365 může být zahrnut Exchange Server, SharePoint Online, Skype for Business, OneDrive for Business a Yammer - ke všem těmto službám přistupují uživatelé i administrátoři v cloudu, tedy z internetu. Balík dále může obsahovat Microsoft Office (Word, Excel, PowerPoint, Outlook, atd.), kde je možnost stáhnout aplikace z internetu pro každý uživatelský účet Office 365 na více zařízení.

Z technického a administrátorského hlediska je částečný rozdíl mezi On-Premise Exchange Serverem a Office 365 ve správě přes PS (PowerShell). U lokálního řešení On-Premise využíváme Exchange Management Shell, který je instalován na každém Exchange Serveru. Office 365 má správu rozdělenou pro AD Azure (Active Directory Azure) a další samostatně pro Exchange Office 365 a s ním spojené služby.

Pro připojení do Exchange Office 365, což se využívá při hybridní konfiguraci, je nutné zadávat administrátorské heslo a jméno. Hybridní konfigurace je kombinace obou řešení – lokálního Exchange Serveru On-Premise a cloudového Office 365. Využívá se, pokud firma plánuje úplný přechod do cloudu, anebo chce rozšířit stávající On-Premise řešení o cloudové aplikace a možnosti.

Princip PowerShell správy je stejný jako u klasického Exchange Serveru, ale není k dispozici tak široké spektrum možností nastavení. Je to zejména proto, že MS (Microsoft) má nastaveny určité parametry, které nelze měnit, a tím si udržují jednotnost a přehlednost z jejich strany. V hybridní konfiguraci se většina úprav dělá přes hybrid server, a proto nás tolik neomezuje méně možných úprav na MS serverech. Ve výpisu 1 uvádím příklad přihlášení právě na MS server přes PowerShell.

```
#Exchange 0365 connection
#$LiveCred = Get-Credentials Admin@customerdomain.com
#$Session = New-PSSession -ConfigurationName Microsoft.Exchange
-ConnectionUri https://ps.outlook.com/powershell/ -Credential $LiveCred
-Authentication Basic -AllowRedirection
#Import-PSSession $Session -DisableNameChecking
```

Výpis 1: Přihlášení na Microsoft server

PowerShell pro Azure AD slouží pro správu cloudového AD, do kterého se pomocí DirSync synchronizují data z lokálního AD. Pro správu je nutné použít Windows Azure Active Directory Module for Windows PowerShell. Samotné přihlášení pak může vypadat jako na výpisu 2.

```
#MSOL connection
#$LiveCred = Get-Credentials Admin@customerdomain.com
#Connect-MsolService -Credential $LiveCred
```

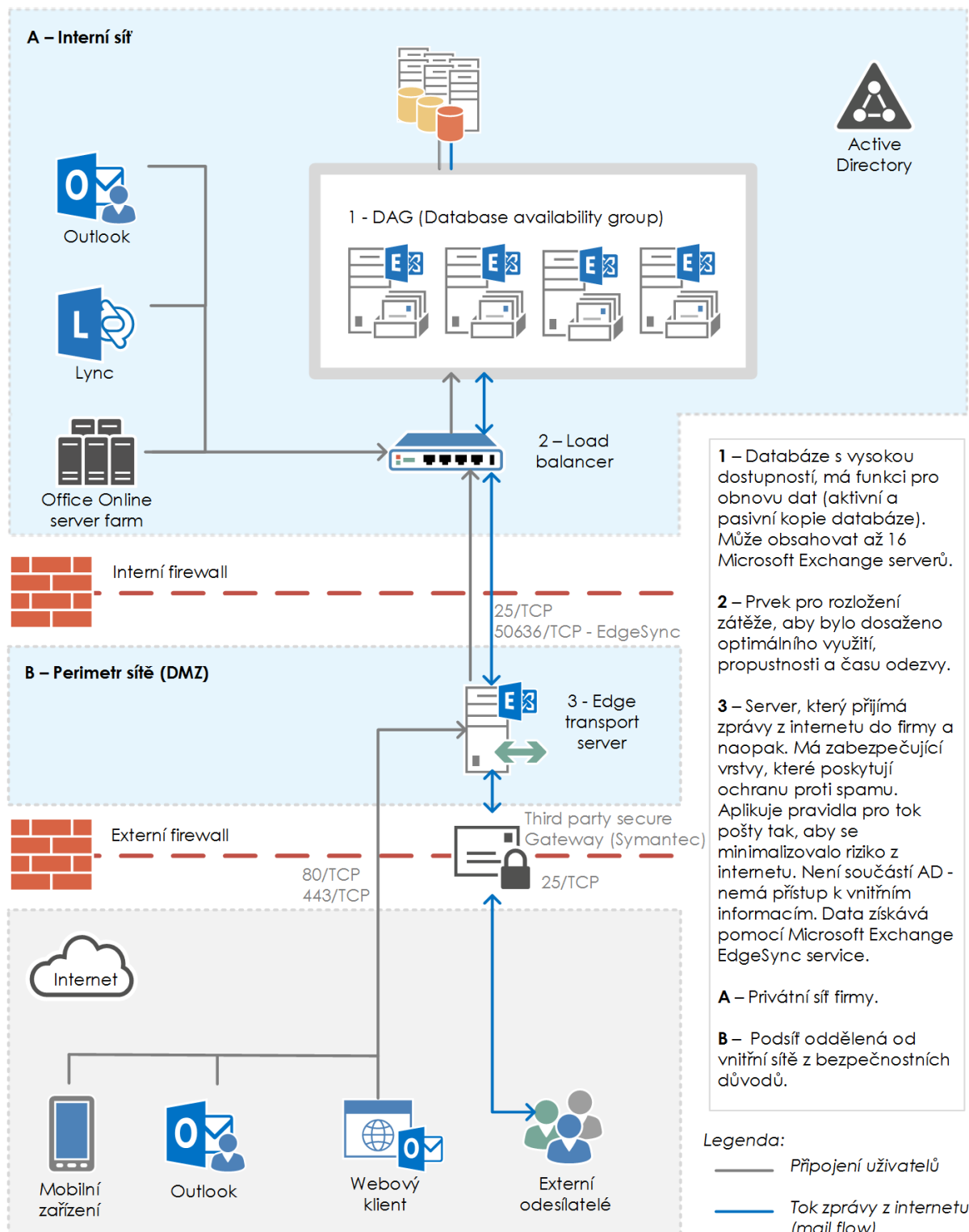
Výpis 2: Přihlášení do PS pro Azure AD

3.5 Srovnání topologií Microsoft Exchange Server a Office 365

Pro nejlepší demonstraci rozdílů v topologii mezi Microsoft Exchange řešeními jsem si vybrala verzi Microsoft Exchange 2016 On-Premise. Starší verze produktu Microsoft Exchange se liší především počtem potřebných fyzických serverů, jelikož bylo nutné využívat více hardwaru a rozložit tak zátěž podle rolí, princip však zůstává stejný. Druhá topologie je cloudové řešení Microsoft Office 365 Exchange, který má ve firemní síti On-Premise pouze servery s interním AD (Active Directory). Výhodou lokálních serverů Active Directory je zjednodušená správa účtů a jejich využití i pro jiné funkce. Mezi ty patří například vnitrofiremní politiky účtů nebo integrace s aplikacemi pro přihlašování s jednotnými přihlašovacími údaji.

Tato řešení jsou zejména ilustrativní, avšak navrhla jsem je tak, aby byla použitelná a reálná a zobrazovala tak co nejlépe odlišnosti. Ve schématech na obrázcích 2 a 3 jsem přímo zahrнула popisy jednotlivých komponent, které jsou pro fungování stěžejní, kvůli jednoduššímu pochopení kompletní topologie a přehlednosti.

3.5.1 Popis topologie MS Exchange On-Premise



Obrázek 2: Topologie prostředí Microsoft Exchange On-Premise

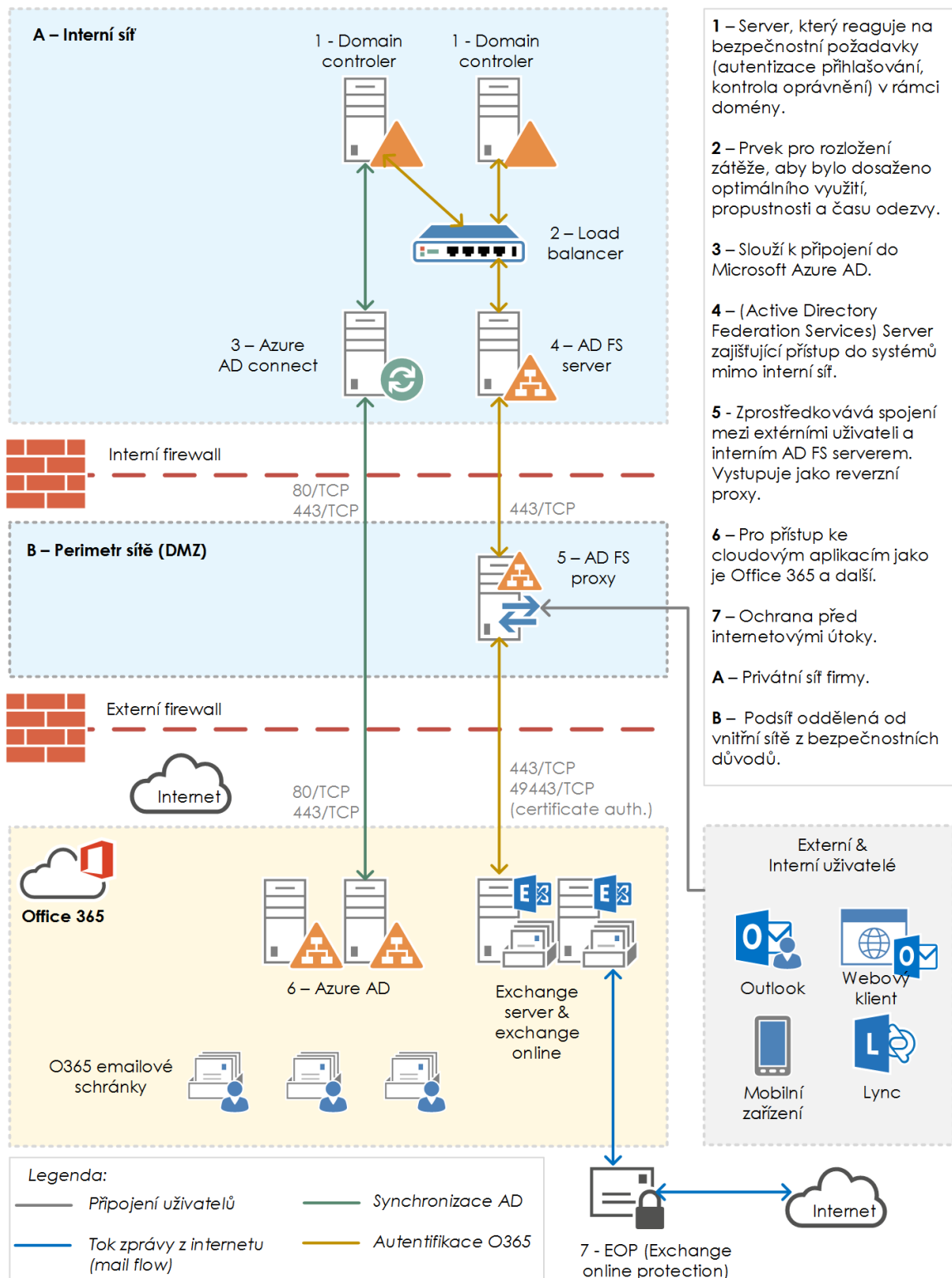
Na schématu (obrázek 2) je topologie prvního řešení, tedy Microsoft Exchange 2016 On-Premise. Firma, využívající tohoto řešení, musí mimo jiné vlastnit Mailbox Servery a Edge Transport Server. Tyto servery jsou nutné k fungování emailové komunikace. Mailbox Servery zastávají veškeré služby spojené s emailovými schránkami a klientským přístupem – z interní sítě se jedná zejména o klientské aplikace Outlook či Lync. Z vnější sítě (internetu) jsou to mobilní zařízení, webová aplikace pro Outlook (Outlook Web App) či jiné. Mailbox Server je základní komponentou pro databáze s vysokou dostupností (Database Availability Group) dále jen DAG. Minimálním počet serverů v DAG jsou 4, ale může jich být až 16. DAG hostí řadu databází a má funkci pro obnovu dat neboli automatické databáze, které dokáží řešit řadu poruch samy, a tudíž klesá riziko poruchy a náročnost na údržbu.

Na druhou stranu roste pořizovací cena hardwaru, která se násobí počtem použitých Mailbox Serverů. Každá firma musí vlastnit Domain Controlery (servery s AD), které jsou součástí interní sítě a nutné pro fungování emailové komunikace ve firmě. Další nezbytně nutnou komponentou je Edge Transport Server, který zajišťuje služby spojené s tokem zprávy do firmy a ven, nebo také zabezpečení či Outlook Voice Access. Z bezpečnostních důvodů se tento server umísťuje mimo interní síť, takzvaně do perimetru sítě, který je oddělen interním i externím firewallem. [4]

Perimetr sítě lze nazvat demilitarizovanou zónou. Tímto je zajištěno, že Edge Transport Server nemá přístup k citlivým datům firmy, například k Active Directory a data získává pomocí služby EdgeSync. Mezi internetem a perimetrem sítě je další zabezpečovací vrstva a to externí firewall poskytovaný třetí stranou. Tyto firewally můžeme nazvat bezpečnostní emailové brány (Messaging Secure Gateways) nebo antivirus/antispam gateway. Kontrolují veškerý tok emailů do vnitřní sítě a z ní. Bezpečnostní emailové brány mohou konfigurovat administrátoři, což byla jedna z mých povinností na odborné praxi. Setkala jsem se s branami třetích stran StaySecure a Symantec Messaging Gateway. Podle potřeb zákazníka lze na branách nastavovat filtry a sledovat veškerý tok emailů, lze dohledávat nedoručené emaily a příčinu jejich nedoručení, dále blokovat specifické odesílatele, IP adresy nebo celé domény a desítky dalších administrátorských funkcí. Každý email je kontrolován bezpečnostní branou podle nastavených pravidel a vyhodnocován, jestli bude doručen či nikoliv. Nedoručené emaily jsou především spamy a zprávy obsahující virus nebo pozměněnou hlavičku zprávy.

Pokud shrnu celou topologii Microsoft Exchange On-Premise, zákazník musí vlastnit veškeré zmíněné servery přímo ve své firmě nebo v datacentru třetí strany a zajišťovat či hradit jejich měsíční údržbu na provoz anebo je mít pronajaté. Dále musí zakoupit licence Microsoft Exchange Serveru pro firmu a všechny další licence, které se vážou na provozování emailové komunikace. S emailem je úzce svázána hlasová komunikace a Lync klient pro rychlé zprávy (*Instant Messaging*), jež je ve firmách také ve velké míře používán. V neposlední řadě musí firma hradit měsíční výdaje za podporu, údržbu a veškeré změny spojené s Exchange Servery a bezpečnostními branami, které nabízí například Tieto.

3.5.2 Popis topologie Office 365



Obrázek 3: Topologie prostředí Microsoft Office 365 s On-Premise AD

Na schématu (obrázek 3) je další řešená topologie – cloudové řešení Microsoft Office 365. Je to velký zlom ve vývoji Exchange Serveru, jelikož firmy již nemusí vlastnit fyzické servery, na kterých je instalován Exchange Server. Nemusí tak řešit kupování drahých licencí a výkonného hardwaru ani údržbu a náklady s tím spojené. Variant topologie Office 365 je více, já jsem navrhla takovou, kde firma vlastní servery s Active Directory (Domain Controller), server pro přístup ke cloudovým aplikacím (Azure AD Connect) a server, který zajišťuje přístup do systémů mimo interní síť (AD FS Server). Pro firmy je výhodné vlastnit tyto servery a to především Domain Controller, jelikož jim umožňuje jednoduchou správu uživatelských účtů ve firmě, autentizaci, udržování vnitrofiremních politik uživatelů a s tím spojené zabezpečení celé firmy. Stejně jako u předchozího řešení (obrázek 2) je v topologii navrhnut takzvaně perimetr sítě, který je oddělen od interní sítě firewallem. V perimetru sítě je umístěn AD FS (Active Directory Federation Services) proxy server, který je určen ke komunikaci mezi AD FS Serverem, který je umístěn v interní síti a externími uživateli. Vystupuje jako reverzní proxy. Z druhé strany je perimetr sítě oddělen externím firewallem, kde se v případě řešení Office 365 jedná o zabezpečení EOP (Exchange Online Protection). EOP je cloudová služba pro filtrování příchozích emailů a chrání firmu proti spamu stejně jako bezpečnostní emailová brána. Je součástí Office 365, a tudíž je poskytovaná Microsoftem, nikoliv třetí stranou. Firmy v O365 však mohou využívat i brány třetích stran jako je Symantec Secure Gateway, StaySecure či jiné.

Dále již firma nemusí vlastnit žádné servery. To nejdůležitější pro emailovou komunikaci, tedy Exchange Server, vlastní Microsoft, který se samozřejmě stará i o jejich celkovou údržbu. V datacentrech Microsoftu jsou ukládány a zálohovány emailové schránky uživatelů. V případě Office 365 zákazník platí měsíční poplatek za licenci na každého aktivního uživatele. V ceně je zahrnuta také podpora, řešení problémů a zabezpečení emailové komunikace EOP. Všechny služby spojené s telekomunikacemi ve firmě jsou v kompletních licenčních balíčcích Microsoftu, firma tak nemusí nakupovat a udržovat vlastní hardware, a tím odpadá starost o údržbu. Firma v Office 365 má navíc v předplatném zahrnuté i veškeré aktualizace na nejnovější verze softwaru.

3.6 Výhody a nevýhody

Obě řešení mají klady i zápory a každé může být výhodnější v jiné situaci. Pro shrnutí a přehlednost vypíšu hlavní rozdíly, výhody a nevýhody obou z nich.

Exchange server On-Premise výhody

- Hardware, tedy fyzické servery patří firmě. Tento bod je zároveň i nevýhodou, jelikož se firma musí starat o údržbu a obměnu hardwaru. Servery může mít firma umístěny také v datacentrech, ale i v takovém případě musí počítat s nemalými výdaji za údržbu.
- Všechna data související s Exchange má firma pod kontrolou a přesně ví, kde jsou data uložena. Firma si určuje politiku přístupů ke svým datům.

- Technickou údržbu zahrnující aktualizace softwaru, hardwaru nebo restart serverů si řídí a kontroluje firma sama a může tak lépe organizovat servisní okno v čase, pro minimalizaci nedostupnosti služby.
- Při výpadku internetu není firma postihnuta nedostupností některých služeb (vnitřní emailová komunikace, SharePoint, Skype for Business).
- Krátké přístupové časy na Exchange Server, jelikož je umístěn v relativní blízkosti koncových uživatelů a není vázán na internet.
- Umožňuje individuální nastavení zabezpečení.

Exchange server On-Premise nevýhody

- Velké prvotní náklady na pořízení hardwaru a softwarových licencí.
- Odpovědnost za vlastní hardware a s ním spojené finance za měsíční údržbu a případnou obměnu. Vlastní odborná nebo placená technická podpora v případě problému.
- Spolehlivost Exchange Serveru je závislá na správné konfiguraci a zkušenosti techniků a administrátorů.

Office 365 Exchange výhody

- Z nabízeného portfolia balíků služeb si každá firma vybere podle svých možností a potřeb a ovlivní tak cenu za měsíční předplatné. Office 365 může zahrnovat Exchange Server, SharePoint, Skype for Business a Office Online služby.
- Odpadá velká prvotní investice za hardware a licence, jako je tomu u On-Premise řešení.
- Všechny služby mají vždy nejaktuálnější verze, v ceně předplatného jsou totiž veškeré nově vydané aktualizace.
- Rychlá a jednoduchá implementace.
- Office 365 slibuje maximální dostupnost, funkčnost a stabilitu produktů, které jsou uživatelům přístupné kdekoli z internetu. Údržba je realizovatelná za provozu.
- Servisní podpora je dostupná přímo od Microsoftu.

Office 365 Exchange nevýhody

- Office 365 se stává nedostupným při výpadku internetu, včetně ostatních online služeb.
- Všechna uživatelská a firemní data jsou uložena v datacentrech Microsoftu, který však nemůže garantovat, kde přesně jsou data lokalizována a to i v případě, že se jedná o data tajná. To může být jedním z faktorů, proč stále některé firmy upřednostňují lokální řešení On-Premise Exchange, kde mají svá data pod úplnou kontrolou.

- Systém předplatného je finančně náročný v čase, to znamená, že za větší časové období je celková suma velká. Musíme však zahrnout fakt, že má firma stále nejnovější software i hardware, neřeší údržbu ani obměnu serverů.

Náročnost a požadavky každé firmy se diametrálně liší. Řešení On-Premise i Office 365 nabízí své silné stránky, se kterými se samozřejmě pojí i negativa a bezchybné řešení, které by fungovalo vždy, zatím neexistuje. Pro mě je důležité znát co nejlépe obě tato řešení, abych byla schopna navrhnout a poradit zákazníkovi ideální řešení.

4 Proces migrace jako moje práce

Na odborné praxi v Exchange týmu jsem se věnovala více typům práce a technickým úkolům. Ze začátku pro mne bylo důležité porozumět základům emailové komunikace, Exchange Serverům a jejich konfiguraci, Active Directory, skriptovacímu jazyku PowerShell, konkrétně pak ovládat jeho rozšíření Exchange Management Shell (PowerShell pro Exchange), bezpečnostním emailovým branám, celkovému zabezpečení a v neposlední řadě také monitorovacím systémům nebo webovým službám spojených s Exchange. Později jsem měla ve firmě také možnost publikovat užitečné informace ohledně emailové komunikace, a tím přispět k eliminaci některých opakujících se dotazů, které musí Exchange tým často řešit.

Jako svůj hlavní projekt jsem si do bakalářské práce vybrala proces migrace z hostovaného Exchange serveru do cloudového řešení Office 365. Jedná se o komplexní telekomunikační projekt, který trvá přibližně osm týdnů. Pokusím se demonstrovat nově nabyté informace z technického i praktického hlediska a shrnout je v této kapitole. Budu se věnovat nejdůležitějším informacím, nikoliv detailnímu postupu. Ve firmách jde o velmi aktuální téma, jak už z pohledu zákazníka, tak poskytovatele.

Součástí projektu migrace je dokumentace, která obsahuje informace o plánování veškerých změn a jejich časový harmonogram, testovací plán, záložní plán, popis dopadu na firmu, popis a konečný výsledek projektu.

Migrace z řešení On-Premise na Exchange Online se liší u každého zákazníka. Hlavní roli zde hrají některé faktory, jako je aktuální verze stávajícího Exchange Server prostředí, ze kterého se bude migrovat, počet emailových schránek, tedy velikost firmy, či jaký balík předplatného je zvolen. Dalším parametrem je také to, jestli bude ve firmě zachována serverová struktura například s Domain Controller servery nebo je požadováno řešení čistě v cloudu.

Moje práce zahrnuje migraci z prostředí On-Premise Microsoft Exchange Server 2007 do Microsoft Office 365, kde se jedná o středně velkou firmu o počtu emailových schránek asi tři tisíce. Zákazníkem byla zvolena varianta balíku předplatného Office 365 Business Essentials, která zahrnuje E-mail s 50 GB poštovní schránkou, 1 TB úložištěm pro ukládání a sdílení souborů - službu OneDrive, HD (High Definition) videokonference - službu Skype for Business a aplikace Office Online pro každého uživatele. V lokálním řešení zůstanou fyzické servery, na kterých bude řešena AD správa. To je výhodné zejména z hlediska širší správy uživatelských účtů ve firmě, udržování vnitrofiremních politik, zabezpečení a propojitelnosti s dalšími systémy a serverovými aplikacemi. Lokálně pak bude umístěn ještě AD FS server, který zajišťuje přístup do systémů mimo interní síť, tudíž do Office 365. Tuto situaci demonstroe mé schéma na obrázku 3.

4.1 Typy migrací

Migrace z existujícího Exchange Serveru do Exchange Online může být realizována několika způsoby. Já jsem volila **fázovou migraci** (*Staged Migration*). Jedná se o migraci využívanou při přechodu z Exchange Server 2003 nebo 2007 prostředí, kde je více než dva tisíce poštovních

schránek. K migraci je zapotřebí Azure AD Connect, o kterém se zmíním později. Druhým typem migrace je **přímá migrace** (*Cutover migration*), která je vhodná při přechodu z prostředí Exchange 2003 až Exchange 2013 a migruje se s méně než dvěma tisíci schránkami. Dalším typem je **IMAP Migrace** nebo **Hybridní nasazení**.

Existují tři typy fázové migrace podle způsobu přihlášení, od toho se pak odvíjí také topologie serverů firmy. V mé práci budu popisovat způsob federace se službou AD FS, základní popis každého typu je následující:

- **Synchronizace hesel** – umožňuje všem uživatelům, aby se ke cloudu přihlašovali stejnými hesly, jaká používají místně. Při synchronizaci hesel se ukládají ani neodesílají hesla v nešifrovaném textu.
- **Předávací ověřování** – Předávací ověřování umožňuje službě Azure AD (Azure Active Directory) ověřovat uživatele prostřednictvím místní infrastruktury identit. Pokud uživatelé chtějí přistoupit ke cloudovým prostředkům, musí se znova přihlásit.
- **Federace se službou AD FS** – umožňuje uživatelům přihlašovat se federovaně, pomocí služby AD FS. Když se uživatelé přihlásí do podnikové sítě, budou mít přístup ke cloudovým prostředkům bez toho, aniž aby museli znova zadávat hesla.

4.2 Fázová migrace

Každé migraci předchází plánování a přípravy, jelikož se jedná o poměrně rozsáhlou změnu ve firemním prostředí. Všem předchází domluvy mezi technikem a zákazníkem, je potřeba seznámit zákazníka s možnými riziky a připravit záložní plány tak, abychom byli schopni řešit výpadky služby v reálném čase. K tomu nám dopomáhá také vhodně naplánovaný harmonogram, abychom významně nenarušili chod celé firmy.

Zvolila jsem způsob federace se službou AD FS z několika důvodů. AD FS má nejvyšší zabezpečení proti hackerským útokům zejména proto, že hodnoty hash hesla jsou ukládána pouze na AD serveru firmy. Hesla, či jiná citlivá data se autentizují a autorizují ve své domácí organizaci a AD FS zajišťuje bezpečný přesun informace (Claim) do druhé organizace, kde se použije.[5] Dále je tento typ vhodný zejména pro větší firmy, které mají několik doménových struktur.

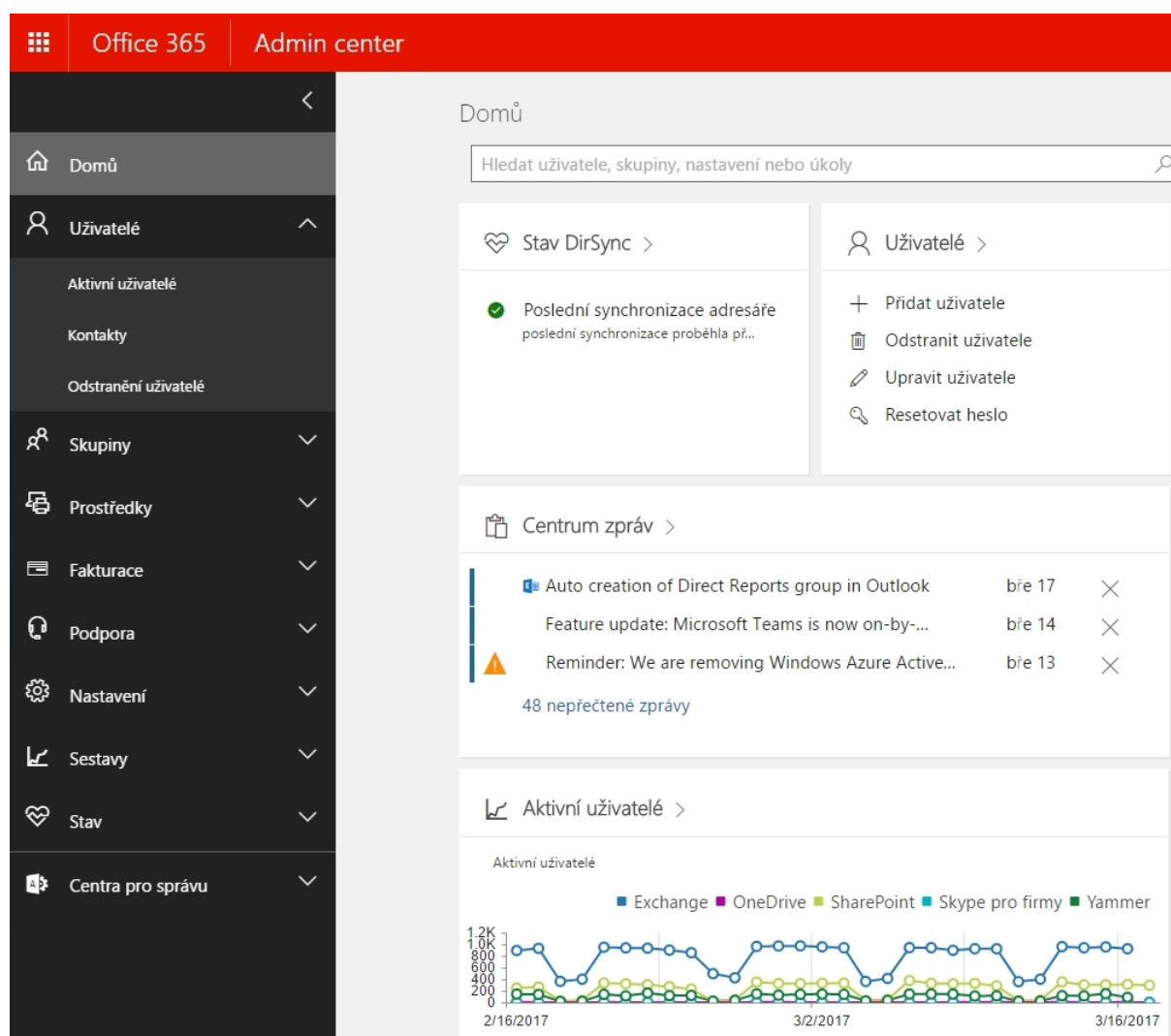
Technická příprava na fázovou migraci spočívá v několika krocích. Základem je konfigurace funkce *Outlook Anywhere*, která umožňuje uživatelům připojit se s Outlook klientem (v mém případě Outlook 2007) k firemní emailové schránce přes internet, bez nutnosti přihlášení do virtuální privátní sítě (VPN). Všichni uživatelé Office 365 využívají Outlook Anywhere stále, je zabezpečen certifikáty SSL (Secure Socket Layer) a pravidly emailové bezpečnostní brány, stejně jako webová aplikace Outlook Web App. Dále je potřeba vytvořit nebo použít již existující administrátorský účet, který má veškerý přístup k místním emailovým schránkám a má povoleno

oprávnění *WriteProperty*. Nazýváme ho *koncový bod migrace*. Přes tento účet pak propojujeme Office 365 s naším lokálním Exchange prostředím.

4.2.1 Účet organizace neboli tenant

Prvotním krokem pro nasazení služeb Office 365 je registrace organizace. Registrací organizace dojde k vytvoření nového účtu organizace, tedy *tenantu*. Tento účet může být v celém cloudovém prostředí, na kterém služby Office 365 běží, jen jeden a je tedy unikátní pro každou firmu. S tímto účtem je následně svázáno vše. Tím mám na mysli, uživatelské účty, provozované domény, předplatné, dostupné služby, a další. Bez tenantu by nemohl být Office 365 vůbec nasazen a provozován.[6]

Jakmile jsem provedla registraci tenantu, dostala jsem informační email s údaji potřebnými pro přihlášení na portál Office 365, který je zobrazen na obrázku 4.



Obrázek 4: Office 365 administrátorský portál

4.2.2 Doména a DNS záznam

Portál má mnoho administrátorských funkcí, můj primární zájem byl vytvořit novou doménu v O365 se jménem určeným zákazníkem. Tento krok konfigurace je intuitivní a velice dobře popsán v samotném rozhraní.

Dále je potřeba vytvořit nový TXT (textový) záznam na DNS (Domain Name System) serveru, abych mohla zadanou doménu v O365 ověřit a verifikovat tak pravost domény. K tomu je nutno přihlásit se na DNS server pod administrátorským účtem a pomocí Správce DNS (DNS Manager) vytvořit nový TXT záznam.

Zvolila jsem zónu, vybrala *Jiné nové záznamy*, v nabídce jsem vyhledala záznam *Text* (TXT) a vyplnila název domény a mailbox server viz obrázek 5. Po dokončení migrace, se podobným způsobem vytváří také MX záznam, který zajišťuje nasměrování emailů do O365. Replikace DNS serveru může trvat až 72 hodin od přidání záznamu, proto musíme s verifikací na portálu O365 počkat.

The image displays two side-by-side screenshots of the MIGRATE.COM web interface for managing DNS records. Both windows have a title bar that reads 'MIGRATE.COM – vlastnosti'.

The left window is titled 'Služba Mail Exchanger (MX)'. It contains the following fields and text:

- Hostitel nebo podřízená doména:** A text box containing '(stejně jako nadřazená složka)'.
- Podle výchozího nastavení používá server DNS název nadřazené domény při vytváření záznamu služby Mail Exchanger. Můžete zadat název hostitele nebo podřízeného serveru, ale ve většině instalací je předchozí pole ponecháno prázdné.**
- Plně kvalifikovaný název domény (FQDN):** A text box containing 'MIGRATE.COM'.
- Plně kvalifikovaný název domény (FQDN) poštovního serveru:** A text box containing 'ms12345678.msv1.invalid' and a 'Procházet...' button.
- Priorita poštovního serveru:** A text box containing '10'.
- Buttons at the bottom: 'OK', 'Storno', 'Použít', and 'Nápověda'.

The right window is titled 'Text (TXT)'. It contains the following fields and text:

- Název záznamu (není-li vyplněno, bude použita nadřazená doména):** A text box containing '(stejně jako nadřazená složka)'.
- Plně kvalifikovaný název domény (FQDN):** A text box containing 'MIGRATE.COM'.
- Text:** A text area containing 'MS=ms12345678'.
- Buttons at the bottom: 'OK', 'Storno', and 'Použít'.

Obrázek 5: Přidání TXT a MX záznamu na DNS server

4.2.3 Azure Active Directory Connect

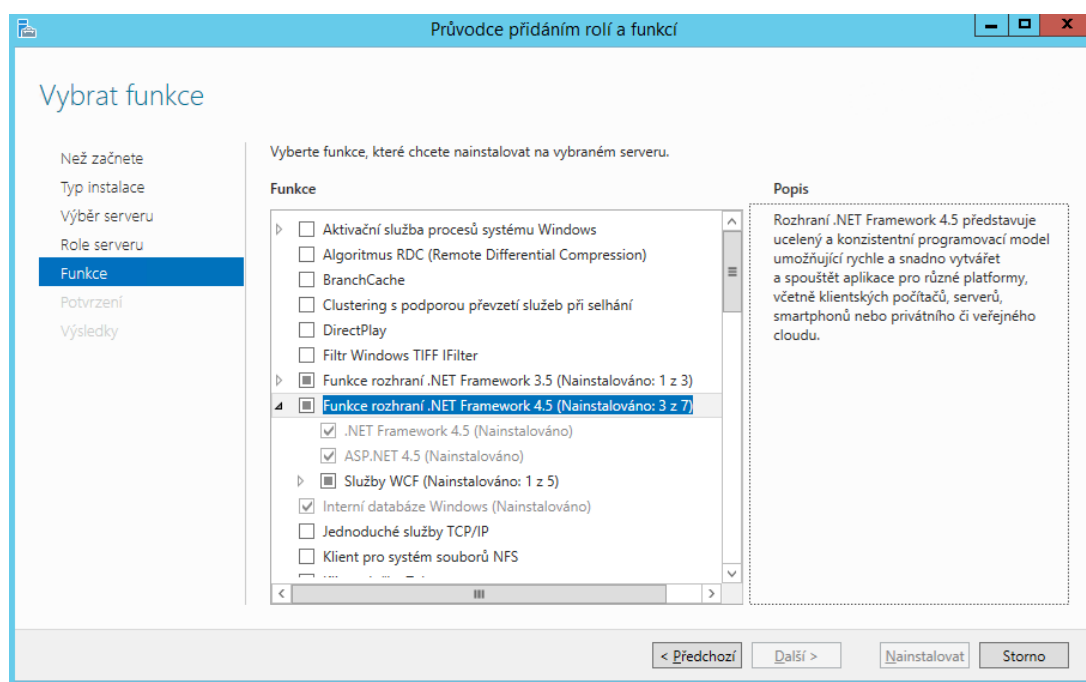
Microsoft Azure AD Connect je zřejmě nejlepší způsob, jak dnes lze propojit lokální AD servery s Azure AD a Office 365, a vytvořit tak místní uživatele v Office 365. Předcházely mu nástroje Azure Active Directory Sync (DirSync) a Azure AD Sync, které plně nahrazuje a od 17. dubna 2017 se stává jediným plně podporovaným nástrojem Microsoftu v této oblasti.[7] **DirSync** synchronizační nástroj byl určen menším zákazníkům s jedním lesem (*forest*). Forest je instance logické struktury Active Directory, který je na nejvyšší úrovni. Dále se forest dělí na nižší instance, jako jsou stromy (*trees*), domény (*domains*) a organizační jednotky (*organization*

units). Uvnitř organizačních jednotek jsou již jednotlivé objekty, například počítače, tiskárny nebo uživatelé. Nástroj **Azure AD Sync** byl naopak určen velkým firmám, které mají rozsáhlé forestové struktury. Tyto dva nástroje jsou již nahrazeny zmíněným Azure AD Connect, který dokáže synchronizovat jak malé, tak i rozsáhlé forestové struktury a navíc nabízí i nově přidané funkce.

Následujícím krokem bylo tedy nastavení Azure AD Connect, který slouží k synchronizaci účtů mezi interním On-Premise Active Directory a Azure AD tenant v našem Office 365. Jedná se o serverovou aplikaci, kterou můžeme instalovat na lokální AD Windows Server ve firmě. U fázové migrace musí mít každá migrovaná emailová schránka odpovídajícího uživatele v Office 365 – to zajišťuje právě práce synchronizačního nástroje.

Jako první jsem v O365 portálu povolila funkci Directory Synchronization, která umožňuje synchronizaci účtů ze strany O365. Doba čekání na povolení funkce může být až 24 hodin.

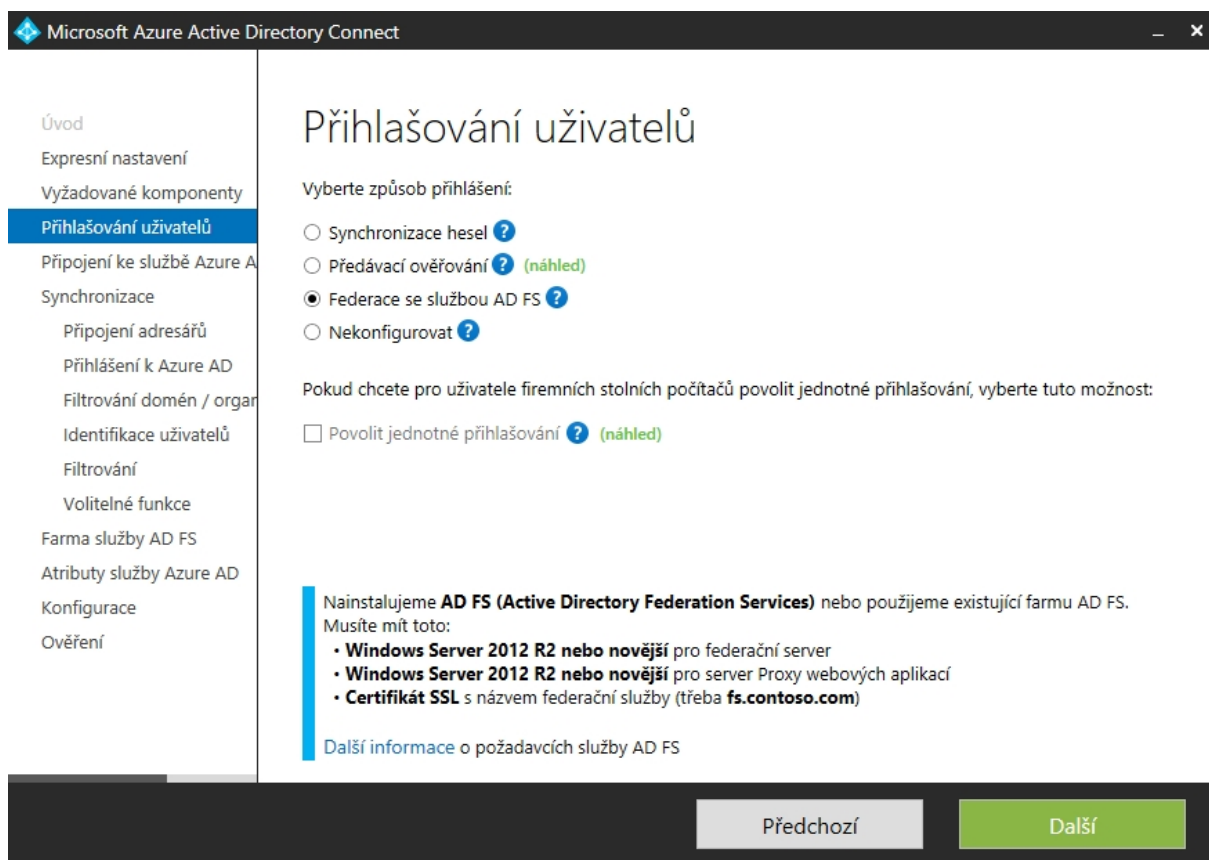
Na AD Serveru firmy jsem nainstalovala nástroj Azure AD Connect, včetně prerekvizity aplikace .Net Framework, kterou jsem instalovala pomocí přidání rolí a funkcí (obrázek 6).



Obrázek 6: Přidání rolí a funkcí na DNS serveru

Po instalaci prerekvizity následuje instalace a spuštění nástroje Azure AD Connect, který má velmi komplexního průvodce instalací, jak lze vidět na obrázku 7. Během instalace se importují uživatelé, kontakty, skupiny i objekty z On-Premise AD na DirSync server, odkud se exportují do O365 předpřipraveného tenantu. Detaily synchronizace a stav průběhu lze kontrolovat v *Synchronization Service Manager on DIRSYNC* nebo v aplikaci *Event Viewer*. Synchronizační nástroj kontroluje nově vytvořené identity a objekty na místním AD serveru a udržuje je aktuální i v administrátorském Centru pro správu Office 365. Synchronizace se provádí v

nastavených časových intervalech nebo ji lze spustit manuálně přes PowerShell pomocí cmdletu *Start-OnlineCoexistenceSync*.



Obrázek 7: Microsoft Azure Active Directory Connect

4.2.4 Soubor CSV

Azure AD Connect synchronizuje zahashovaná hesla z lokálního AD do prostředí Office 365. Dalším důležitým krokem k migraci je vytvoření CSV souborů. Jedná se o textové soubory, které obsahují informace o uživatelských účtech, které budu migrovat z On-Premise na Exchange Online.

Obsah souboru musí být vytvořen ve tvaru *EmailováAdresa,Heslo,ZměnaHesla*. Každý uživatel musí být na samostatném řádku. Hodnota v poli *ZměnaHesla* může mít hodnotu TRUE nebo FALSE. Určuje, zda bude při prvním přihlášení po migraci vyžadována po uživateli změna hesla. CSV souborů je obvykle více, jelikož každý může obsahovat maximálně tisíc řádků, tedy přesně 999 uživatelských účtů. První řádek souboru obsahuje názvy jednotlivých atributů. Vzor CSV souboru je ve výpise 3.

```
EmailAddress,Password,ForceChangePassword  
Name.Surname@vsb.cz,Heslo123,True
```

Výpis 3: CSV soubor

Struktura CSV souborů se liší u různých typů migrací. Pokud se přechází například z hybridního řešení do Office 365, CSV soubor obsahuje pouze seznam emailových adres, které budou migrovat do cloudu a další atributy nepotřebuje.

4.2.5 Centrum pro správu Exchange

Následně jsem pracovala v centru pro správu Exchange, které je již zobrazeno na obrázku 1. Přes rozhraní se vytváří koncový bod migrace, který obsahuje informace o místním účtu určeném pro správu. Dále již následuje migrace emailových schránek, která se takzvaně *fázuje* a spouští se přes záložku *migrate*. Vždy se migruje po jednom CSV souboru, takže migrace má tolik migračních dávek, kolik máme připravených CSV souborů. V centru pro správu Exchange můžeme kontrolovat status na řídicím panelu.

Po dokončené migraci změníme místní emailové schránky na uživatele s podporou pošty – toto nastavení nám umožní spravovat již cloudové uživatele z místního On-Premise AD Serveru a zachovat proxy adresy. Změna je možná přes prostředí Exchange Management Shell.

4.2.6 Migrovaná data

Ačkoliv je migrace provedena správně, musí administrátoři počítat s tím, že některá data při migraci zaniknou. Samozřejmě se nejedná o klíčová data, avšak v tabulce 1 uvedu přehled.

Tabulka 1: Přenesená a zaniklá data při migraci

Přenesená data	Zaniklá data
Emailové zprávy a konverzace	Skupiny s oprávněními (Security Groups)
Nastavená pravidla pro zprávy a kategorie	Dynamické distribuční seznamy
Kalendáře	Systémové emailové schránky
Nastavení „Out-of-Office“	Oprávnění „Send-As“
Delegace emailové schránky	Veškeré přijaté zprávy větší než 150 MB
Úkoly	Dumpster (zabezpečení dat)
Kontakty	
Nastavená práva k emailovým schránkám	

Díky tomu, že víme, která data při migraci zanikají a která nikoliv, můžeme je dopředu zálohovat. Zaniklá data následně v cloudovém prostředí aplikujeme pomocí O365 PowerShellu použitím scriptu nebo manuálně.

Veškeré přijaté zprávy větší než 150 MB exportujeme do PST (Personal Storage Table) souboru. Tyto soubory se používají právě pro ukládání osobních dat z aplikace Microsoft Outlook a lze je po migraci importovat do uživatelské poštovní schránky. Manuálně pomocí O365 PowerShellu se dají dále nastavit zaniklá „Send-As“ oprávnění (výpis 4).

```
Add-RecipientPermission -Identity "mailbox name" -AccessRights SendAs -Trustee  
name.surname@vsb.cz
```

Výpis 4: Nastavení „Send-As“ oprávnění

Problém nastává s dynamickými distribučními seznamy, které cloudové prostředí O365 neumí. Jsou to AD objekty, které jsou vytvořeny a používány za účelem urychlení správy a hromadného zasílání emailových zpráv pracovním skupinám. Pokud zákazník na jejich užívání trvá, mohou zůstat umístěny na hybridním serveru, odkud budou využívány.

4.2.7 Výsledek migrace

Díky přípravám a preciznosti se mi podařilo přesunout všechny emailové schránky z lokálního prostředí do cloudového Microsoft Office 365 podle plánu. Migrace a následné využívání služeb novodobého cloudového řešení má pro firmu značné přínosy.

Hlavním benefitem je menší finanční zatížení firmy, která již nemusí zajišťovat údržbu fyzických Exchange serverů ani techniky samotné. V nákladech za měsíční předplatné jsou navíc zahrnuty veškeré aktualizace i nové verze aplikací bez dalších investic, takže veškerý software je takzvaně *up-to-date* (aktuální). Uživatelé se mohou připojit odkudkoliv z internetu a jsou jim tak jejich aplikace mnohem lépe přístupné kdykoliv potřebují. Dalším přínosem je rozšiřitelnost – firma může libovolně expandovat a navyšovat počet emailových schránek, jelikož není omezena hardwarem. S využíváním cloudových služeb souvisí také redukce plánovaných výpadků, způsobených nutnou údržbou serverů, jelikož všechna údržba se již řeší za provozu, nezávisle na dni nebo hodině.

5 Bezpečnost a ochrana dat

Dalším tématem, kterému jsem se na bakalářské praxi věnovala, je bezpečnost, která je nedílnou součástí emailové komunikace zejména proto, že každý uživatel požaduje mít svá data šifrovaná a v bezpečí před útoky, spamem či nevyžádanou poštou z internetu. Dnešní řešení se snaží zajistit perfektní ochranu, ale hraje tady velkou roli právě práce administrátorů. Formy ochrany dat jsou dostupné, jak u lokálních řešení, tak v cloudu. U lokálních Exchange Serverů, jsou využívány převážně bezpečnostní emailové brány.

5.1 Bezpečnostní emailová brána

K zabezpečení emailové komunikace mezi internetem a perimetrem sítě firmy, se u lokálních řešení používají bezpečnostní emailové brány třetích stran (znázorněno na obrázku 2). Firemní infrastruktura je chráněna před nevyžádanou poštou (spam), škodlivým softwarem (malware), útoky z internetu, dále dokáže filtrovat obsah na základě zadaných pravidel, šifrovat emaily nebo blokovat odesílatele.

Ačkoliv dnes už lokální řešení Exchange server 2013 a všechny vyšší verze zahrnují vlastní ochranu, bezpečnostní emailové brány se stále využívají, jelikož jsou specializovanější a poskytují větší jistotu a funkčnost. Natavení jsou administrátorsky flexibilní, protože každá firma má jiné nároky na svou infrastrukturu. Bezpečnostní brány mají samozřejmě i výchozí nastavení pro rozlišování nevhodných nebo nebezpečných zpráv. Administrátoři mají detailní přehled nad tokem emailů do vnitřní sítě a z ní, díky bezpečnostním emailovým branám můžeme kontrolovat nežádoucí zprávy a vytvářet nová pravidla. Na své praxi jsem pracovala nejvíce s bezpečnostní branou SMG (Symantec Messaging Gateway). Společnost Symantec má široké portfolio produktů v oblasti antispamové ochrany a zabezpečení dat.

5.2 Práce s bezpečnostní emailovou branou

SMG zobrazuje v první řadě vždy aktuální statistiky příchozí pošty. Čistých, tedy doručených zpráv bývá kolem 25% z celkového objemu (tabulka 2). To znamená, že bezpečnostní brána zachycuje velké množství nevyžádané pošty. Velkou část filtrů tvoří právě administrátory nastavená pravidla, která jsou ve statistikách označena jako *bad reputation*, tedy zachycené emailové zprávy zakázaných odesílatelů, domén nebo dokonce celých IP adres poštovních serverů. Tato pravidla jsou vždy specifická pro každou firmu.

Jedním z mých úkolů bylo dohledávání a následné blokování emailových účtů, domén či IP adres, na základě přijaté nevyžádané pošty. Jako první je důležité zkontrolovat a identifikovat odesílatele. Všechny informace o samotné zprávě, odesílateli a příjemci nebo poštovních serverech, kterými zpráva prošla, se zapisují do hlavičky každé emailové zprávy. K tomu jsem používala MX Lookup, který vypisuje MX (Mail Exchange) záznamy pro doménu, umožňuje diagnostiku poštovního serveru, kontrolu reverzního DNS záznamu a měří dobu odezvy.

Tabulka 2: Přehled zpráv s hrozbami redukovánými SMG za 30 dní

Zprávy	Počet	%
Zprávy s jednou hrozbou	18,374,636	72,3
Zprávy s více hrozbami	221,681	0,9
Celkový počet zpráv s hrozbami	18,596,317	73,2
Čisté zprávy	6,825,619	26,8
Celkový počet zpráv	25,421,936	100
Hrozby	Počet	%
Porušování obsahu	465,201	2,5
Malware (škodlivý software)	1,728	<0,1
Neplatní příjemci	1,568,465	8,3
Reputace (zakázání odesílatelů)	15,296,216	81,2
Spamy	1,495,491	7,9

Dále lze kontrolovat MX záznamy či IP adresy v *blacklist* databázi. Blacklist databáze obsahuje záznamy o nebezpečných odesílatelích. Po ověření nevhodného odesílatele pomocí MX Lookup zablokují příjem emailových zpráv od dané emailové adresy, domény nebo IP adresy, podle rozsahu možného či vzniklého problému.

Opačným problémem je blokování správných odesílatelů, kvůli výchozímu nastavení brány. Tento problém nastává většinou při obsahu nevhodných slov nebo příloh, které brána vyhodnotí jako spam. Řešení je přidat odesílatele do *whitelist* databáze. Whitelist databáze obsahuje záznamy o odesílatelích (emailové adresy), jejichž zprávy obcházejí antispamovou kontrolu.

Dále jsem na bezpečnostních branách vyhledávala určité emailové zprávy z důvodu nalezení problému, proč nebyla zpráva doručena či jiných. Emailová bezpečnostní brána zachycuje veškerý tok zpráv a udržuje logy administrátorům přístupné po dobu třiceti dní. Branou prochází obrovské množství emailů, proto lze pro vyhledávání využít vhodně zadaných filtrů podle příjemce, odesílatele, rozmezí časového období, předmětu zprávy a mnoha dalších. Bezpečnostní brány jsou spolehlivým ukazatelem při problémech s poštovními servery, je možno sledovat fronty zpráv, a pokud se na poštovním serveru z nějakého důvodu zprávy hromadí, lze to snadno identifikovat. V neposlední řadě jsem pracovala s karanténami doručených zpráv, kde se hromadí zprávy, které jsou zachyceny spamovou filtrací, ale nejsou ani doručeny, ani smazány. Podle potřeby je možnost manuálně tyto zprávy uvolnit, tedy nechat doručit do emailové schránky příjemce.

6 Další úkoly v rámci odborné praxe

Na odborné praxi v rámci vypracování bakalářské práce jsem pracovala a učila se řešit výše zmíněné projekty, jako je kompletní migrace, avšak nedílnou součástí bylo také řešení jednotlivých menších problémů, které byly na denním pořádku. Exchange tým zajišťuje technickou podporu svým zákazníkům, požadavky a problémy k nám tak přicházely každý den. Většina problémů je velmi specifických a je potřeba řešit je dle každého jednotlivého uživatele. Je zapotřebí dokázat pracovat se všemi používanými prostředními Exchange Server nebo různými typy emailových bezpečnostních bran, jelikož zákazníci nemají unifikovaný vzor, který by splňovali. Asi jediný univerzální nástroj pro správu je EMS (Exchange Management Shell).

EMS je postaven na Microsoft PowerShell, jedná se o skriptovací platformu, která používá jako rozhraní rozšířenou příkazovou řádku. Díky EMS dokáží technické a administrátory spravovat právě Exchange Server pomocí příkazů zvaných *cmdlets*. Cmdlet, nebo také commandlet je tvořen jmennou konvencí Sloveso-PodstatnéJméno, příkazy jsou intuitivní a dobře se pamatují.[8] Mnohé problémy je pohodlnější a přehlednější řešit v grafickém administrátorském rozhraní Exchange Management Console (pro Exchange Server 2007 a 2010) a Exchange Administration Center (pro Exchange Server 2013), ale není to vždy nejefektivnější způsob například pro hromadné úpravy. Pomocí EMS jsem řešila problémy, jejichž řešení by bylo v administrátorském rozhraní zdlouhavé, nepřehledné či nemožné. Postupně jsem se s EMS učila pracovat a korektně používat cmdlets, které při špatném použití mohou způsobit hodně škody, třeba i v celém prostředí. Velice užitečným tak pro mě byl parametr *-WhatIf*, který se zadává na konec příkazového řádku. Díky tomu se příkaz nespustí, nýbrž vypíše, co se po jeho zadání stane. Je to výborný testovací trik, který mne naučil správně pracovat s EMS.

Dále ukázkově zmíním, jaké příkazy jsem vytvořila a jak s nimi pracovala. Tím demonstruji další dílčí úkoly a náplň odborné praxe, kterou jsem ve firmě vykonávala.

6.1 Out of office

Funkcionalita *out of office*, je vhodná například v situacích, kdy zaměstnanec nebude delší dobu k dispozici v práci. Může si tak nastavit na svou emailovou schránku zasílání automatické odpovědi s informacemi o jeho dovolené. Automatická odpověď se dá nejlépe nastavit přímo v emailovém klientu Outlook nebo jiném. V případě, že zaměstnanec zapomene odpověď nastavit a již není přítomen, může ji na žádost jeho nadřízeného přidat dle požadavku. Samozřejmě je nutná správa přes EMS, kvůli zákazu přístupu přímo do poštovní schránky uživatele bez jeho svolení.

```
#Set-MailboxAutoReplyConfiguration "name.surname@vsb.cz" -AutoReplyState  
Scheduled -EndTime "01/07/2017 06:00:00" -InternalMessage "<br><br>I am on  
holiday.<br><br>" -ExternalMessage "<br><br> I am out of the office, I  
will be back at 01/07/2017.<br><br>"
```

Výpis 5: Nastavení out of office

Díky takovému příkazu, jako je na výpisu 5, nastavím hned několik parametrů najednou. Parametr *-EndTime* určuje, do kdy se bude automatická odpověď odesílat. Pokud by se zaměstnanec vrátil do práce dříve, při zapnutí se jej Outlook dotáže, zda si přeje odesílání odpovědi vypnout předčasně. Dalšími často používanými parametry jsou *-InternalMessage* a *-ExternalMessage*. Tyto slouží k rozlišení odpovědi pro interní a externí odesílatele.

Zprávy do *-InternalMessage* a *-ExternalMessage* se přes EMS vkládají a upravují v jazyce HTML (HyperText Markup Language) či XHTML (eXtensible HyperText Markup Language) v podobě tagů a jeho atributů. Použitý tag `
` slouží na zalomení řádku v HTML a `
` v XHTML.

6.2 Auto-mapping

Auto-mapping je funkce Exchange, díky které lze automaticky otevírat poštovní schránky, na které má uživatel úplná přístupová oprávnění (full access). Jedná se většinou o sdílené poštovní schránky, pro které se auto-mapping povoluje či zakazuje. Tato funkce se nastavuje výhradně v EMS a přes administrátorské rozhraní nelze spravovat.

Řešila jsem například zrušení auto-mappingu pro určitého uživatele na sdílenou poštovní schránku, kde mu však měla být zanechána úplná přístupová oprávnění. Prvním krokem je úplně zrušit přístup, ať už v EMS či v rozhraní. Dále se přístup znova povolí v EMS, ale již s parametrem *-Automapping \$false*, který nám zakáže právě auto-mapping (výpis 6).

```
#Add-MailboxPermission -Identity "shared mailbox name" -User name.surname@vsb.cz -AccessRight FullAccess -InheritanceType All
-Automapping $false
```

Výpis 6: Nastavení auto-mapping

6.3 Přístupová oprávnění

Nastavování přístupových oprávnění je jedním z nejčastějších požadavků ze strany uživatelů. Exchange team řeší především práva ke sdíleným poštovním schránkám, schránkám prostředků, složkám či kalendářům. Sdílená poštovní schránka (*Shared Mailbox*) je schránka určená pro skupinu uživatelů, kteří k ní mohou mít různé úrovně oprávnění, o kterých se zmíním níže. Emailová schránka prostředků (*Resource Mailbox*) může být využívána jako schránka k místnosti nebo vybavení a slouží k jejich rezervaci.

Na sdílenou schránku existují tři různá oprávnění, první z nich je **plný přístup** (*Full Access*), který garantuje úplnou kontrolu nad schránkou a jejím obsahem. Uživatel může odesílat i mazat emaily a měnit nastavení, má stejná práva jako majitel schránky. Druhé je **odesílat jako** (*Send As*), což uživateli umožňuje odesílat emaily pod jménem sdílené složky, nemůže však zprávy ze schránky mazat ani je jinak upravovat. Poslední možností je **odesílat jménem** (*Send on*

Behalf), to umožňuje odesílat zprávy pod jménem sdílené schránky, ale vždy příjemce uvidí také jméno opravdového odesílatele.

Pro oprávnění na složky emailové schránky můžeme přidělit **delegovaný přístup** (*Delegate Access*). Podle potřeby se nám zase nabízí tři úrovně oprávnění, které lze přidělit. **Editor** je nejvyšší stupeň oprávnění, lze delegovat veškeré složky a emaily s právy je měnit i mazat. Stupeň **autor** může číst stávající emaily a měnit i mazat emaily a složky, které sám vytvoří, může tak přidávat například i schůzky do kalendáře. Nejnižším stupněm přístupu k osobní emailové schránce je **reviewer**, který může pouze číst příchozí emaily, nikoliv je upravovat, mazat či odesílat.

Přístupová oprávnění lze nastavovat přes grafické rozhraní. V případě, že přiřazujeme jednomu uživateli více práv nebo několika uživatelům práva na několik objektů, není to vždy nejrychlejší způsob. Za takových okolností je mnohem efektivnější využít EMS a vhodných cmdletů. Setkala jsem se například s problémem, kdy jsem měla povolit práva na několik kalendářů sdílených schránek pro jednoho uživatele. Prvním krokem je vytvoření textového souboru přímo na serveru, kde jsem si vypsala přesné názvy sdílených schránek, což je zobrazeno ve výpisu 7.

```
#mailboxes=Get-content D:\Desktop\fil0094\mailboxes.txt
#mailboxes | %{Get-MailboxFolderStatistics $_ -folderscope calendar | select
    identity}
#mailboxes | %{Get-Mailbox $_ | fl *primary*}
```

Výpis 7: Výpis sdílených schránek

První řádek ve výpisu 7 načte názvy sdílených schránek, které potřebujeme, další dva jsou pro výpis názvu kalendářů daných schránek a výpis primárních SMTP adres. Použitý znak `$_` doplňuje automaticky do příkazu všechny řádky z textového souboru. Primární SMTP adresy si uložím do textového souboru ve tvaru: *sharedmailbox@vsb.cz:\Calendar*.

```
#permissions=Get-content D:\Desktop\fil0094\permissions.txt
#permissions | %{Add-MailboxFolderPermission -identity $_ -User name.
    surname@vsb.cz -AccessRights Author}
```

Výpis 8: Přiřazení práv

Podle výpisu 8 přiřadíme ke všem kalendářům sdílených schránek stejná práva pro jednoho uživatele v několika krocích. V případě, že se jedná o desítky kalendářů, nám použití EMS ušetří mnoho času, jelikož správa přes rozhraní je sice pohodlná a přehledná, ale v některých případech opravdu pomalá.

6.4 Úložiště

Dalším typickým požadavkem je omezování či rozšiřování velikosti úložiště emailové schránky (Storage Quota) nebo archivu (Archive Quota). Ačkoliv je jednodušší nastavit kvóty přímo v

Exchange rozhraní, není od věci, vždy si aktuální nastavení překontrolovat přes EMS. Mnoho firem totiž dodržuje své standardy, a tak je nejlepším způsobem vypsání si nestandardní kvóty schránek či archivů, pokud existují, aby nedošlo k chybnému rozšíření. Pokud se nám vypíše různá nastavení velikostí, je jasné, že firma nedodržuje v tomto žádné pravidlo a emailovou schránku či archiv můžeme rozšířit ad libitum.

```
#Get-MailboxDatabase | fl name, *quota*  
#Get-Mailbox -ResultSize unlimited | ?{$_ .UseDatabaseQuotaDefaults -ne $true} |  
    ft *prohibit*, *issue* -AutoSize
```

Výpis 9: Výpis kvót

První příkaz ve výpisu 9 slouží k prohlédnutí všech databází a vypsání, jaké jsou na nich kvóty, druhý příkaz vypisuje právě emailové schránky s nedodrženým nastavením.

7 Zhodnocení znalostí a dovedností

Praktickou bakalářskou práci považuji za velký přísun nabytých informací v jiné formě, než je tomu u studia. Teorie se prolíná s praxí, a tak lze znalosti efektivně využívat, modifikovat a vybírat ty nejlepší metodiky v konkrétních situacích při řešení konkrétních problémů.

7.1 Znalosti získané v průběhu studia

Při absolvování praxe jsem využila znalosti získané v průběhu studia a to zejména z oblasti správy serverů, virtuálních serverů, telekomunikací, sítí, zabezpečení a informatiky. Díky tomu, že jsem i volitelné předměty směřovala tímto směrem, již jsem měla základní znalosti o Windows a Linux serverech při nástupu do firmy. Právě v předmětu **Správa Windows systémů** jsem se poprvé setkala se serverovým prostředím jak prakticky, tak teoreticky, což mi umožnilo rychleji se začlenit do celkové problematiky emailové komunikace. Dobrým základem pro mne tvořily znalosti v administraci serverů, správě diskových kvót, zálohování dat, správě služeb DNS a DHCP, a v neposlední řadě architektura a správa uživatelů či skupin v Active Directory, do kterého je Exchange prostředí integrováno. Seznámila jsem se se skriptovacím jazykem PowerShell, jehož rozšíření Exchange Management Shell jsem na praxi využívala poměrně často.

Z dalších předmětů **Počítačové sítě** a **Praktikum komunikačních sítí I** jsem využila znalosti z oblasti protokolů (SMTP, IMAP nebo POP3), jež se vážou k elektronické komunikaci. Seznámila jsem se s fungováním a konfigurací DNS serveru, významem DNS záznamů a sítěmi obecně. Užitečný přehled z oboru telekomunikací jsem získala také díky předmětu **Spojovací soustavy**. Tento předmět je převážně zaměřen na vývojové etapy ústředěn a hlasovou komunikaci, avšak dnešní integrace zahrnuje do emailové komunikace i *voicemail*, což je systém, jež umožňuje zasílání hlasových emailových zpráv. Dalším propojeným předmětem s mou praxí byl **Přenos dat**, kde jsem se naučila, jak fungují šifrovací a kompresní metody, způsob přenosu či zabezpečení zpráv. Bezpečnost celkově je dnes velmi žádoucí, a tak není pochyb, že je u emailové komunikace stěžejní.

Znalosti ze studia mi pomohly především v tom, že jsem získala širší přehled o využívaných technologiích v telekomunikacích, o tom, jak fungují servery, internetové protokoly nebo zabezpečení. Předměty obsahují celá spektra informací, a tak není možné věnovat se jen jednomu tématu do detailů v rámci jednoho předmětu. Od toho pro mne byla právě odborná praxe, kde jsem prohlubovala své znalosti v oboru emailové komunikace, a to jak teoretické, tak praktické.

7.2 Znalosti scházející v průběhu odborné praxe

Se zahájením odborné praxe jsem se sama snažila nastudovat co nejlépe a detailně problematiku emailových zpráv, fungování Exchange prostředí a Exchange serverů. Technologie v této oblasti jdou rychle kupředu, takže je někdy obtížné vyhledat relevantní informace. Díky práci v týmu, jsem mohla konzultovat veškeré dotazy se zkušenými pracovníky. Obecnějších informací se mi

souvisle dostávalo taktéž ze studia, jelikož nejpřínosnější předměty pro mne byly právě ve třetím ročníku.

Scházející znalosti tak pro mne byly právě odborné informace týkající se Exchange serverů, topologií, administrátorských funkcí, správy Exchange prostředí nebo toku emailových zpráv. Naučila jsem se, jaké možnosti a problémy jsou spojené s emaily, co to jsou emailové bezpečnostní brány či jak se pracuje s nežádoucí poštou a daleko více. Nakonec jsem měla možnost zapojit se do komplexního projektu migrace a poznat blíže současné cloudové technologie. Díky přechodu mezi prostředími jsem studovala historii a vývoj Exchange prostředí, rozdíly mezi implementacemi jednotlivých řešení a odlišnosti ve využívaných technologiích. Cloud computing se dnes dostává do mnoha technických oborů, takže jsem velmi ráda, že jsem se cloudové technologii mohla věnovat právě na odborné praxi a zjistit, jaké výhody a nevýhody přináší v této oblasti.

7.3 Celkové zhodnocení

Se znalostmi ze studia jsem v důsledku velmi spokojená, jelikož mi daly kvalitní přehled v daném oboru. Na odborné praxi jsem prohloubila znalosti v oblasti, kterou jsem si vybrala a snadněji porozuměla celkovému objemu informací. Práce na opravdových problémech a projektech mne naučila správně aplikovat teorii a pracovat v týmu. Díky této zkušenosti pro mne bude rozhodně jednodušší orientovat se v daném oboru.

Závěr

S výběrem odborné praxe pro vypracování bakalářské práce jsem velice spokojená. Prohloubila jsem své znalosti v oblasti emailové komunikace praxí i studiem, začlenila jsem se do týmu specialistů a dokázala jsem samostatně pracovat na zadaných úkolech a projektech. Díky tomu, že jsem podrobně sepsala chybějící dokumentaci, jsem zjednodušila průběh dalším podobným projektům a podílela jsem se na úspěšné realizaci migrace. Tento projekt bude využit pro rozšíření služby pro další, mimo jiné i české zákazníky. Kromě práce na projektu jsem publikovala ve firmě článek do firemního zpravodaje o funkcích a aplikacích spojených s emailovou komunikací, které mnozí uživatelé neznají, a rozšířila tak povědomí například o využívání webové cloudové aplikace Outlook Web App nebo používání zabezpečeného emailu při odesílání důvěrné pošty.

Začlenění a několika týdenní práce na projektu byla pro mne velkým přínosem a cennou zkušeností v rámci praxe. Naučila jsem se týmové spolupráci, jelikož komunikace je základem při řešení složitých problémů. Aplikovala jsem své znalosti v pracovním prostředí, kde jsem se setkala s novými technologiemi, jako je cloud computing. Měla jsem možnost porovnat výhody a nevýhody lokálních Exchange řešení a cloudového řešení Office 365 a navrhnout jejich topologie. Pochopila jsem, jak fungují řešení firem v rámci emailové komunikace, jak se dají upravovat podle potřeb zákazníka a jak mohou být variabilní. Naučila jsem se práci se servery a pracovala s různými administrátorskými nástroji pro správu. V neposlední řadě jsem se naučila pracovat s bezpečnostními emailovými branami, nastavovat pravidla pro příjem pošty či dohledávat a rozpoznávat nevyžádanou poštu.

Velkou výhodou absolvování praktické bakalářské praxe je pro mne nabídka dále pokračovat v práci ve firmě a motivace pokračovat v navazujícím studiu. Díky cenným pracovním zkušenostem se mohu lépe orientovat na trhu práce a dále rozšiřovat své zkušenosti.

Literatura

- [1] Tieto Czech s.r.o., O nás [online]. 2017, [cit. 2017-04-01]. Dostupné z: <https://www.tieto.cz/tieto-o-nas>
- [2] Microsoft TechNet, Exchange Server Updates [online]. 2017, [cit. 2017-04-01]. Dostupné z: <https://technet.microsoft.com/library/hh135098.aspx>
- [3] Microsoft Office, porovnání plánů a cen pro Office 365 [online]. 2017, [cit. 2017-04-01]. Dostupné z: <https://products.office.com/cs-cz/business/compare-office-365-for-business-plans>
- [4] Microsoft TechNet, Edge Transport servers [online]. Poslední revize 29. 9. 2016. [cit. 2017-04-01]. Dostupné z: [https://technet.microsoft.com/en-us/library/bb124701\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/bb124701(v=exchg.160).aspx)
- [5] Saloň Zbyněk. Microsoft TechNet Blog, AD FS (1) - Terminologie [online]. 14. 1. 2016, [cit. 2017-04-01]. Dostupné z: <https://blogs.technet.microsoft.com/technetczsk/2016/01/14/adfs-1-terminologie/>
- [6] Havránek Zdenek. Svět Office 365, Co je to „Tenant“? [online]. 26. 4. 2016, [cit. 2017-04-01]. Dostupné z: <http://www.svetoffice365.cz/domains/svetoffice365.cz/2016/04/26/co-je-to-tenant/>
- [7] Microsoft TechNet, Deploy Office 365 Directory Synchronization (DirSync) in Microsoft Azure [online]. Poslední revize 10. 2. 2017. [cit. 2017-04-01]. Dostupné z: <https://technet.microsoft.com/en-us/library/dn635310.aspx>
- [8] Rouse Margaret. TechTarget, Microsoft Exchange Management Shell (EMS) [online]. Poslední revize říjen 2012, [cit. 2017-04-01]. Dostupné z: <http://searchexchange.techtarget.com/definition/Microsoft-Exchange-Management-Shell-EMS>